PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) **International Patent Classification:** **H02H 3/05, G06F 15/177, H04L 1/22**	**A1**	(11) **International Publication Number:**	**WO 00/51216**
		(43) **International Publication Date:**	31 August 2000 (31.08.2000)

(21) **International Application Number:** PCT/US00/05086

(22) **International Filing Date:** 24 February 2000 (24.02.2000)

(30) **Priority Data:**
09/258,028 25 February 1999 (25.02.1999) US

(60) **Parent Application or Grant**
LODGENET ENTERTAINMENT CORPORATION [/]; (). SLEMMER, Michael, W. [/]; (). ZINGER, David, F.; ().

Published

(54) **Title: METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED COMMUNICATION OVER A NETWORK LINK**
(54) **Titre: PROCEDE ET APPAREIL ASSURANT UNE COMMUNICATION ININTERROMPUE SUR UNE LIAISON DE RESEAU**

(57) Abstract

A system for providing uninterrupted communication over a network link includes a multi-port switch that is connected to a first network portion and a second network portion (Fig. 1) that are communicating with one another. The multi-port switch is also connected to a separate server unit, such as a firewall computer. The switch is configured to direct communication signals flowing between the first network portion and the second network (Fig. 1) portion through the separate server unit for processing during normal operation. When the separate server unit fails, however, the switch is reconfigured so that communications bypass the separate server unit. In a preferred embodiment, a Ethernet switch having virtual local area network (VLAN) capability is used.

(57) Abrégé

L'invention concerne un système assurant une communication ininterrompue sur une liaison de réseau, qui comporte un commutateur multi-accès relié à une première partie du réseau et à une deuxième partie du réseau (Fig. 1) qui communiquent entre elles. Le commutateur multi-accès est également relié à un serveur distinct, tel qu'un ordinateur pare-feu. Le commutateur est configuré pour diriger des signaux de communication entre la première partie du réseau et la deuxième partie du réseau (Fig. 1) par l'intermédiaire du serveur distinct en vue d'un traitement, lors d'une exploitation normale. Cependant, en cas de défaillance du serveur, le commutateur est reconfiguré de sorte que les communications contournent ce serveur distinct. Dans un mode de réalisation préféré, on utilise un commutateur Ethernet possédant une capacité de réseau local virtuel (VLAN).

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H02H 3/05, H04L 1/22, G06F 15/177 — A1

(11) International Publication Number: **WO 00/51216**

(43) International Publication Date: 31 August 2000 (31.08.00)

(21) International Application Number: PCT/US00/05086

(22) International Filing Date: 24 February 2000 (24.02.00)

(30) Priority Data:
09/258,028 25 February 1999 (25.02.99) US

(71) Applicant: LODGENET ENTERTAINMENT CORPORATION [US/US]; 3900 West Innovation Street, Sioux Falls, SD 57107 (US).

(72) Inventor: SLEMMER, Michael, W.; Apartment 310, 400 East 13th Street, Sioux Falls, SD 57104 (US).

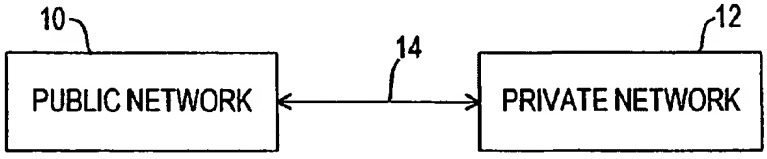
(74) Agents: ZINGER, David, F. et al.; Sheridan Ross P.C., Suite 1200, 1560 Broadway, Denver, CO 80202-5141 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED COMMUNICATION OVER A NETWORK LINK

(57) Abstract



A system for providing uninterrupted communication over a network link includes a multi-port switch that is connected to a first network portion and a second network portion (Fig. 1) that are communicating with one another. The multi-port switch is also connected to a separate server unit, such as a firewall computer. The switch is configured to direct communication signals flowing between the first network portion and the second network (Fig. 1) portion through the separate server unit for processing during normal operation. When the separate server unit fails, however, the switch is reconfigured so that communications bypass the separate server unit. In a preferred embodiment, a Ethernet switch having virtual local area network (VLAN) capability is used.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Description

5

10

15

20

25

30

35

40

45

50

55

METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED COMMUNICATION OVER A NETWORK LINK

FIELD OF THE INVENTION

The invention relates generally to communication networks and, more specifically, to devices for ensuring uninterrupted service in a communication network.

BACKGROUND OF THE INVENTION

Communication networks generally comprise a number of communication nodes that are interconnected using some form of communication medium. For example, a local area network (LAN) is a communication network that includes a number of user terminals in a relatively localized area that are interconnected amongst each other by a network medium such as a twisted pair or coaxial cable. Communication networks can also be connected to other communication networks so that users of one connected network can communicate with users of another connected network. An example of this is the Internet which consists of a large number of individual networks that are connected to one another through a high capacity backbone medium. Individual communication networks can also be subdivided into a number of subnetworks that each consist of a subgroup of the total nodes in the network. For example, a large corporation having many different buildings may maintain a different subnetwork for each building. The subnetworks are then interconnected to form the corporate network. The individual subnetworks are often separately addressable entities that can be individually managed.

Oftentimes, it is desirable to insert a server or other type of network device within an individual link in the network so that all communications through that link pass through the server. An example of this would include the insertion of a firewall device within the connection path between two networks or subnetworks, such as between a private network and the Internet. A firewall device is essentially a filter that controls the type of information that can flow into or out of an individual network. For example, a corporation whose corporate network is connected to the Internet may install a firewall within the connection to prevent external entities from having access to the corporation's internal files. The corporation's firewall can also be used to control which extra-corporate resources the corporations employees will have access to.

A network server that is located within an individual link of a network can create a problem if the server fails during network operation. That is, the failure will generally sever the connection between the nodes on either side of the network link. If a firewall device fails, for example, the two networks attached thereto will no longer be able to communicate with one another. Many times, such network links are critical to an entity's business activities and must operate without interruption. For this reason, many businesses are reluctant to install servers within these critical links. Failure to install such servers (such as, for example, a firewall) may compromise network security, which can produce equal or greater harm to the entity.

Therefore, a need exists for a method and apparatus that allows uninterrupted service through a network link having a server, even if the server fails.

SUMMARY

The present invention relates to a method and apparatus for providing uninterrupted communication over a network link that includes in-line processing functionality, such as a firewall device. The system includes a switch that can be used to bypass the in-line processing functionality should the functionality fail. In one embodiment, backup functionality is provided to perform the in-line processing when a failure of the original processing functionality is detected. The system also includes a controller for monitoring the in-line processing functionality and for reconfiguring the switch when a failure is detected. The invention can be advantageously implemented, for example, to provide uninterrupted, secure access to a private communications network using a firewall device or similar apparatus.

In a preferred embodiment of the invention, the switch is an Ethernet switch having virtual local access network (VLAN) capabilities. VLAN capabilities allow port groups to be defined that control how external entities connected to the switch will be interconnected with one another. In addition, switching modes can generally be defined that each include a different combination of port groupings. In accordance with the present invention, the mode of the Ethernet switch is changed when a failure of an in-line processing unit has been detected. This mode change effectively bypasses the failed unit so that communications is substantially uninterrupted.

BRIEF DESCRIPTION OF THE DRAWINGS

Figs. 1 and 2 are block diagrams illustrating typical networking arrangements between a public network and a private network;

Fig. 3 is a block diagram illustrating a system in accordance with one embodiment of the present invention;

Fig. 4 is a block diagram illustrating a system in accordance with another embodiment of the present invention;

Fig. 5 is a block diagram illustrating a system in accordance with yet another embodiment of the present invention.

DETAILED DESCRIPTION

The present invention relates to a system for providing uninterrupted service through a network link having an in-line server. That is, even if the in-line server fails, communications over the network link are not severed. Thus, the system allows servers (such as firewall devices) to be used within critical network links without fear of losing the network link. The system includes a switching device that allows the server to be bypassed if and when a server failure occurs. In a preferred embodiment, the server bypass function is automatic and operates in substantially real time so that critical communications through the link are minimally affected. The system has particular application in networks utilizing Ethernet technology.

The principles of the present invention will be described in conjunction with an Internet firewall embodiment. It should be appreciated, however, that the principles of the present invention have application in any network configuration where a first network portion is connected to a second network portion by a network link that includes an in-line server through which communications must pass. For example, in one embodiment, the inventive principles are used to provide uninterrupted communication between two subnetworks within a single network that are interconnected via a connection device within the network. It should also be noted that the figures set forth herein generally use the same reference numerals to describe the same or similar functionality.

Fig. 1 is a block diagram illustrating a typical networking scenario wherein a private network 12 is connected to a public network 10 via an inter- network connection 14. The

private network 12 can include, for example, a network within a corporation that allows employees of the corporation to communicate and share resources with one another. The public network 10 can include any network that can be accessed by the public, such as the Internet. The inter-network link 14 represents the communication path between the networks 10, 12 and can include, for example, a connection from the private network 12 to the Internet backbone. Such a connection can be direct or through an Internet Service Provider (ISP).

For security reasons, a manager of the private network 12 may decide that access to the private network 12 from the public network 10 is to be limited. In such cases, the manager will generally place a firewall device 16 somewhere within the inter-network link 14, as illustrated in Fig. 2. In general, a firewall device is a filter that only allows certain information to pass from an input port to an output port. All other information is generally discarded. Firewall devices can be implemented in software, hardware, or a combination of the two. Often, firewall devices are implemented using personal computers that are preprogrammed with the appropriate firewall routines. Firewall devices are generally placed "in-line" within a network link so that all communications on the link pass through the firewall device. As can be appreciated, this "in-line" configuration can create problems should the firewall device 16 fail. Most notably, such a failure could cut off all communications through the implementing network link.

Fig. 3 is a block diagram illustrating a system 20 for providing an uninterrupted connection between two networks in accordance with one embodiment of the present invention. It should be appreciated that the blocks shown in Fig. 3 and other block diagrams herein are functional elements that do not necessarily correspond to discrete hardware elements. For example, two or more of the associated functions may be implemented in software within a single digital processor. As illustrated, the system 20 includes a switch 22, a controller 24, and a firewall device 16 and is interposed within a inter-network link 14 between a public network 10 and a private network 12. The system 20 is capable of providing an uninterrupted connection between the public network 10 and a private network 12, regardless of the condition of the firewall device 16. The switch 22 includes a number of input/output ports for receiving and transmitting signals. At least one of the ports is connected to the public network 10, at least one is connected to the private network 12, and at least one other port is connected to the firewall device 16. The controller 24 is coupled to

the switch 22, via control line 36, for controlling the operation thereof. The controller 24 is also coupled to the firewall device 16, via sense line 40, for sensing a present operational condition of the firewall device 16.

During normal operation, the switch 22 is operative for directing all communications between the public network 10 and the private network 12 to the firewall device 16 for processing. If the firewall device 16 fails, however, the switch 22 provides a direct communication path between the two networks 10, 12 until the failure has been remedied. The controller 24 monitors the condition of the firewall device 16 and configures the switch 22 in accordance therewith. That is, during normal operation, the controller 24 sends information/instructions to the switch 22 that configures the switch to direct communications through the firewall device 16. When the controller 24 detects that the firewall device 16 has failed, it sends information/instructions to the switch 22 that reconfigures the switch 22 to enable a bypass of the firewall device 16. The controller 24 can then signal a network operator that the firewall device 16 needs to be repaired or replaced.

The controller 24 can include virtually any type of device that is capable of sensing a condition and generating an appropriate control signal in response thereto. In a preferred embodiment, the controller 24 is implemented within a digital processing device, such as a general purpose microprocessor or a digital signal processor. The controller 24 can be a separate unit from the switch 22 or it can be an integral part of a larger switch assembly. The controller 24 can sense a failure of the firewall device 16 in any of a number of different ways. For example, as shown in Fig. 3, a sense connection 40 can be provided between the controller 24 and the firewall device 16 that allows the controller 24 to directly monitor/ measure one or more performance related characteristics of the firewall device 16. The controller 24 can then determine whether the firewall device 16 has failed based on these characteristics. Another method for determining whether a firewall failure has occurred involves monitoring the signals going into and out of the firewall device 16. The controller 24 can do this by monitoring, for example, the port(s) of the switch 22 that is coupled to the firewall device 16. If it is determined that nothing is being passed by the firewall device 16, it can be assumed that a failure has occurred. In one technique, the controller 24 performs a "test" on the firewall device 16 by sending a test signal into the device 16 via the switch 22. The test signal is one that should pass through the firewall device 16 in a known manner. For

example, the test signal could be a packet that should pass through the firewall device 16 and emerge with a particular destination address in a header portion. If the signal does not pass through the firewall device 16 in the expected manner, the controller 24 can use this as evidence of a failure. As can be appreciated, many other methods for detecting firewall failures can also be used in accordance with the present invention. In a preferred approach, the controller 24 will only register failures that will result in a serious reduction in throughput through the firewall device 16. That is, less serious failures that only reduce throughput slightly will be ignored.

The switch 22 can include any form of switch that is capable of performing the requisite bypass in response to a control signal. The switch 22 can include either mechanical or electrical switching elements or the switching function can be implemented in software. In a preferred embodiment of the invention, as illustrated in Fig. 4, an Ethernet switch 38 having virtual local area network (VLAN) capability is used. The Ethernet switch 38 has a number of input/output ports 26-29 that are used to receive/transmit information from/to attached entities. In the illustrated embodiment, a first port 26 is connected to the private network 12, a second port 27 is connected to the public network 10, and a third and fourth port 28, 29 are connected to the firewall device 16. That is, the third port 28 of the switch 38 is connected to a first port 30 of the firewall device 16 and the fourth port 29 of the switch 38 is connected to a second port 31 of the firewall device 16.

The VLAN capability of the Ethernet switch 28 , in general, allows a user to define a number of different VLAN groups for the Ethernet switch 38 that control how external entities connected to the Ethernet switch 38 are interconnected through the switch 38. Each of the VLAN groups corresponds to one or more of the available input/output ports of the switch 38, thus allowing all external entities connected to those ports to communicate with one another through the switch 38. If two ports are not associated with a common VLAN group, then the external entities attached to those ports will not be able to communicate with one another through the Ethernet switch 38 (although they may be able to communicate with one another via a connection outside the Ethernet switch 38). The Ethernet switch 38 will also preferably allow switching "modes" to be defined. Each of the switching modes will consist of a different arrangement of VLAN groups. The controller 24 can then change the

current mode of the Ethernet switch 38 by delivering an appropriate control signal to the Ethernet switch 38 via control line 36.

In the preferred embodiment, a first switch mode is defined for use when the firewall device 16 is operating properly and a second switch mode is defined for use when the firewall device 16 has experienced a failure. In the first mode, a first VLAN group is defined that includes the second and third ports 27, 28 of the switch 38 and a second VLAN group is defined that includes the first and fourth ports 26, 29 of the switch 38. Thus, the public network 10 is linked to the first port 30 of the firewall device 16 and the private network 12 is connected to the second port 31 of the firewall device 16. Communications between the public network 10 and the private network 12 must therefore take place through the firewall device 16 which appropriately filters the communications. In the second mode, a third VLAN group is defined that includes the first port 26 and the second port 27 and a fourth VLAN group is defined that includes the fourth port 29. Thus, the public network 10 is given direct access to the private network 12 and the firewall device 16 is bypassed. It should be noted that the first and second VLAN groups will normally be deactivated when the second switch mode is enabled. It may be desirable to include the third port 28 of the Ethernet switch 38 within the third VLAN group so that users within the private network 12, for example, can monitor the condition of the firewall device 16 (e.g., determine when it is again operational). In a preferred embodiment, the controller 24 will simply indicate a mode number to the switch 38 to appropriately configure the switch 38 based on current conditions. In an alternate embodiment, the controller 24 must indicate to the switch 38 which of the switch ports are to be interconnected within each VLAN group at a particular point in time.

As can be appreciated, some private networks are not able to allow full public access to the network, even for a short period of time. For example, a corporation may maintain important business information on its network that it does not want to be accessible by its competitors. Fig. 5 is a block diagram illustrating a system 50 that is capable of providing uninterrupted, firewall-protected communication between two networks in accordance with one embodiment of the present invention. As illustrated, the system 50 is similar to the previously described embodiment with the addition of a backup firewall device 52 for use when the first firewall device 16 fails. The backup firewall device 52 includes a first port 54 that is connected to a fifth port 44 of the Ethernet switch 38 and a second port 56 that is

connected to a sixth port 46 of the Ethernet switch 38. In addition, the backup firewall device 52 can also be connected to the controller 24 via a sense line 48. The backup firewall device 52 can be identical to the first firewall device 50 or, to reduce implementation costs, a less sophisticated device may be implemented.

With reference to Fig. 5, during normal operation, the controller 24 configures the Ethernet switch 38 to direct all communications between the public network 10 and the private network 12 through the firewall device 16. When the controller 24 detects a failure of the firewall device 16, the controller 24 reconfigures the Ethernet switch 38 to all communications through the backup firewall device 52. A first mode can be defined that includes a first VLAN group comprising the second and third ports 27, 28 of the Ethernet switch 38 and a second VLAN group that includes the first and fourth ports 26, 29 of the switch 38. A second mode is defined that includes a third VLAN group comprising the second and fifth ports 27, 44 of the switch 38 and a fourth VLAN group that includes the first and sixth ports 26, 46 of the switch 38. When the controller 24 detects a failure of the first firewall device 16, it instructs the Ethernet switch 38 to change from the first switch mode to the second switch mode. The backup firewall device 52 then takes over the filtering function. When the first firewall device 16 has been repaired or replaced, the Ethernet switch 38 can be returned to the first switch mode. As can be appreciated, any number of backup firewall devices can be provided in accordance with the principles of the present invention.

Although the present invention has been described in conjunction with its preferred embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. For example, as described previously, the principles of the invention can be used to ensure connectivity in any network situation that involves an in-line server device. This may include, for example, servers that are located between sub-networks in a single overall network. Such modifications and variations are considered to be within the purview and scope of the invention and the appended claims.

Claims

What is claimed is:

1. A system for use in providing uninterrupted communication between a first network portion and a second network portion, comprising:

a server unit for processing signals input into said server unit, said server unit including an output for outputting processed signals;

a multi-port switch having a first port connected to the first network portion, a second port connected to the second network portion, and a third port connected to said server unit; and

a controller, operatively coupled to the multi-port switch, for configuring said switch during normal operation so that communications between said first network portion and said second network portion are input into said server unit for processing, said controller including an apparatus for reconfiguring said switch, in response to a predetermined occurrence, so that communications between said first network portion and said second network portion are not input into said server unit for processing.

2. The system, as claimed in claim 1, wherein:

said predetermined occurrence includes detection of a failure of said server unit by said controller.

3. The system, as claimed in claim 1, wherein:

said controller includes a monitor for monitoring said server unit to determine whether a failure has occurred within said server unit.

4. The system, as claimed in claim 1, wherein:

said server unit includes a firewall machine.

5. The system, as claimed in claim 1, wherein:

said multi-port switch includes an Ethernet switch having virtual local access network (VLAN) functionality

6. The system, as claimed in claim 1, wherein:

said controller includes a digital processing unit.

7. The system, as claimed in claim 1, wherein:

said controller is integrally associated with said multi-port switch.

8. The system, as claimed in claim 7, wherein:

said controller is located within a housing of said multi-port switch.

9. The system, as claimed in claim 1, further comprising:

a backup server unit coupled to a fourth port of said multi-port switch.

10. The system, as claimed in claim 9, wherein:

said apparatus for reconfiguring said switch reconfigures said switch so that communications between said first network portion and said second network portion are input into said backup server unit for processing.

11. The system, as claimed in claim 1, wherein:

said apparatus for reconfiguring said switch reconfigures said switch so that communications between said first network portion and said second network portion are transferred without processing within said system.

12. The system, as claimed in claim 1, wherein:

said first network portion is located within a first network and said second network portion is located within a second network, wherein said second network is different from said first network.

13. The system, as claimed in claim 1, wherein:

said first network portion and said second network portion are both subnetworks of a common network.

14. A system for use in providing uninterrupted communication between a first network portion and a second network portion, said system comprising:

a switch having a plurality of ports, wherein a first of said plurality of ports is coupled to the first network portion and a second of said plurality of ports is coupled to the second network portion, said switch permitting port groups to be defined that each include a subset of said plurality of ports, wherein two external entities are only capable of directly communicating with each other through said switch if the two external entities are each connected to respective ports of said switch that are within a common port group, said switch having a first configuration comprising first and second port groups and a second configuration comprising a third port group, wherein said third port group is different from said first and second port groups;

a server unit having a first server port and a second server port, said first server port being connected to a third of said plurality of ports and said second server port being

connected to a fourth of said plurality of ports, wherein said server unit is operative for processing signals propagating between said first server port and said second server port; and

a controller, coupled to said switch, for changing a configuration of said switch from said first configuration to said second configuration in response to a predetermined occurrence.

15. The system, as claimed in claim 14, wherein:

said first port group includes said second port and said third port of said switch and said second port group includes said first port and said fourth port of said switch.

16. The system, as claimed in claim 15, wherein:

said third port group includes said first port and said second port of said switch.

17. The system, as claimed in claim 15, further comprising:

a backup server unit having a third server port and a fourth server port, said third server port being connected to a fifth of said plurality of ports and said fourth server port being connected to a sixth of said plurality of ports, wherein said backup server unit is operative for processing signals propagating between said third server port and said fourth server port;

wherein said third port group includes said second port and said fifth port of said switch, said second configuration further comprising a fourth port group including said first port and said sixth port of said switch.

18. The system, as claimed in claim 14, wherein:

said switch includes an Ethernet switch having virtual local area network (VLAN) capability.

19. The system, as claimed in claim 18, wherein:

each of said port groups comprises an individual VLAN grouping.

20. The system, as claimed in claim 14, wherein:

said predetermined occurrence includes detection of a failure of said server unit.

21. The system, as claimed in claim 14, wherein:

said server unit includes a firewall machine for use in filtering signals flowing therethrough.

22. The system, as claimed in claim 14, wherein:

said controller is not accessible from at least one of said first network portion and said second network portion.

23. The system, as claimed in claim 14, wherein:

said third port group further comprises said third port of said switch.

24. A method for use in providing secure access to a first network portion from a second network portion utilizing an Ethernet switch, said Ethernet switch having at least three ports, a first port being connected to the first network portion, a second port being connected to second network portion, and at least one port being connected to a firewall machine, said firewall machine including an ability to filter signals that are input into said firewall machine so that only authorized signals are allowed to pass to an output of said firewall machine, said method comprising the steps of:

first configuring said Ethernet switch so that communications flowing between the first and second network portions are directed through the firewall machine for processing;

monitoring said firewall machine to detect failures within said firewall machine; and

second configuring said Ethernet switch, when a failure has been detected in said firewall machine, so that communications flowing between the first and second networks bypass the firewall machine.

25. The method, as claimed in claim 24, wherein:

said Ethernet switch includes virtual local area network (VLAN) functionality, wherein said at least one port includes a third port and a fourth port connected to said firewall machine; and

said step of first configuring includes enabling a first VLAN grouping and a second VLAN grouping, wherein said first VLAN grouping includes said second port and said third port and said second VLAN grouping includes said first port and said fourth port.

26. The method, as claimed in claim 25, wherein:

said step of second configuring includes enabling a third VLAN grouping including said first port and said second port of said switch.

27. The method, as claimed in claim 26, wherein:

said third VLAN grouping includes at least one of said third port and said fourth port.

28. The method, as claimed in claim 24, further comprising:

providing a backup firewall machine that is coupled to at least one fifth port of said Ethernet switch, wherein said step of second configuring includes configuring said Ethernet switch so that communications flowing between the first and second network portions are directed through the backup firewall machine for processing.

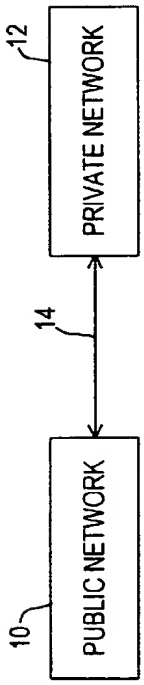

12
PRIVATE NETWORK
14
PUBLIC NETWORK
10

FIG. 1

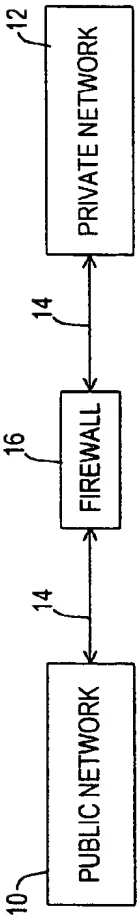

12
PRIVATE NETWORK
14
16
FIREWALL
14
PUBLIC NETWORK
10

FIG. 2

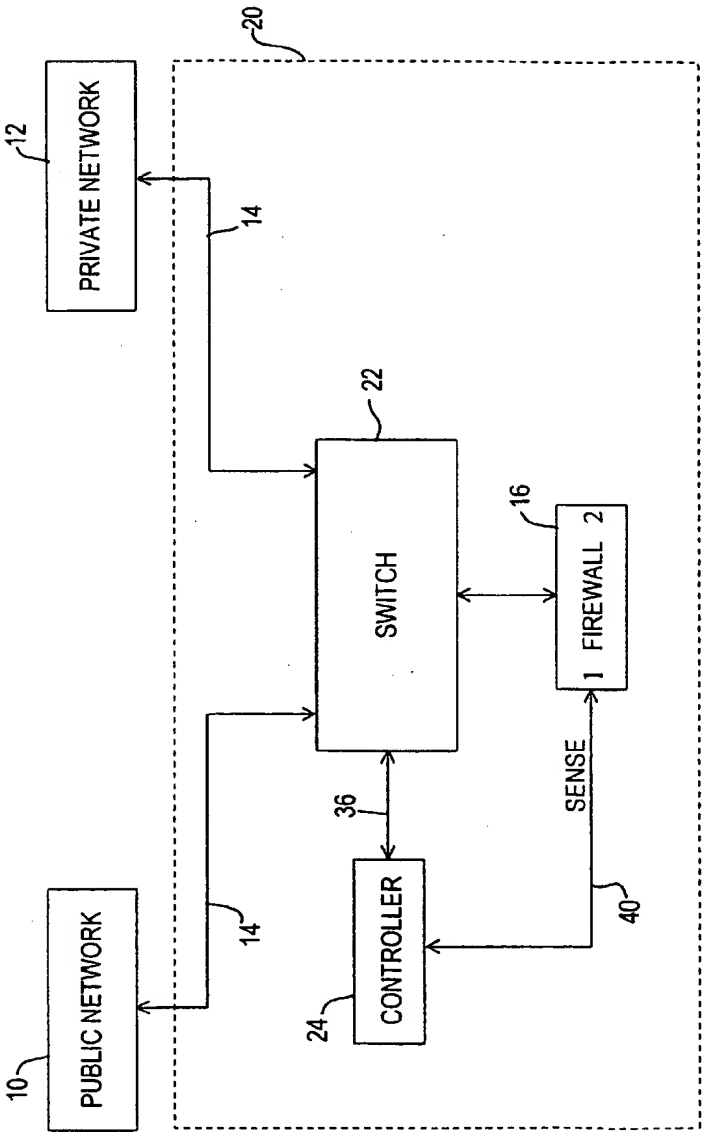

20
12
PRIVATE NETWORK
14
22
SWITCH
16
FIREWALL 2
SENSE
36
40
CONTROLLER
24
14
PUBLIC NETWORK
10

FIG. 3

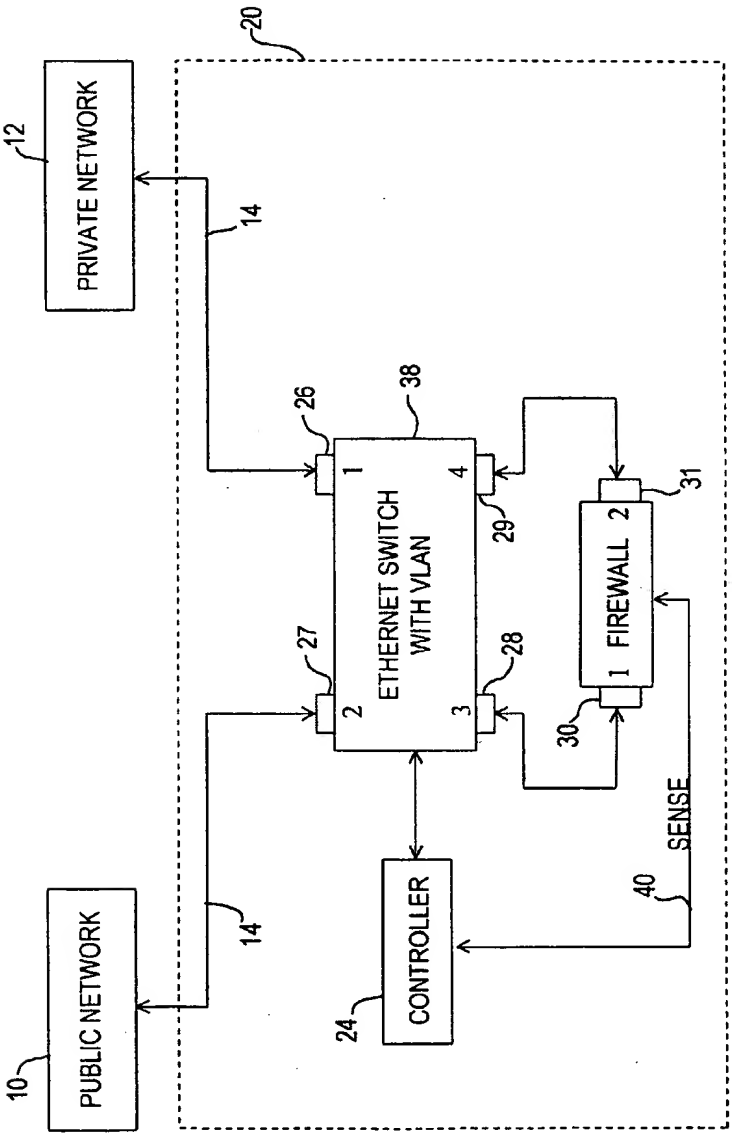

20
12
PRIVATE NETWORK
14
26
38
1
4
ETHERNET SWITCH
WITH VLAN
2
3
27
28
29
31
1 FIREWALL 2
30
SENSE
40
14
CONTROLLER
24
10
PUBLIC NETWORK

FIG. 4

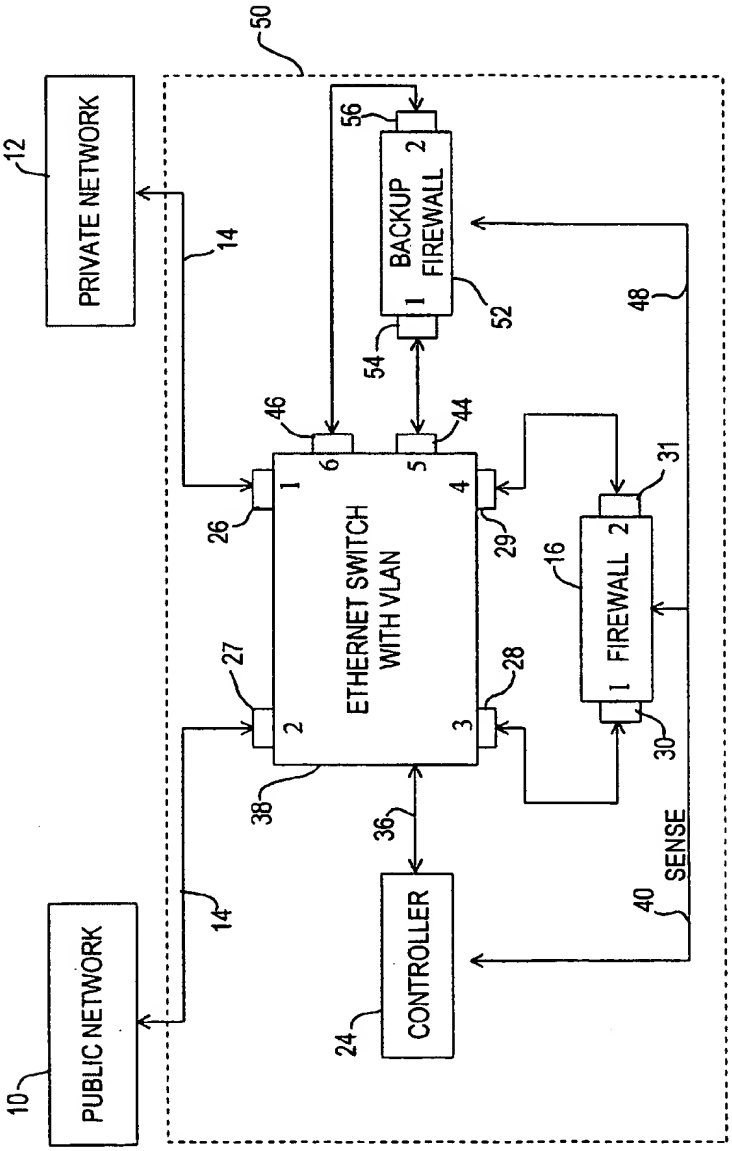

50
PRIVATE NETWORK
12
14
BACKUP FIREWALL
56
2
1
52
48
54
46
44
6
5
1
4
26
29
31
ETHERNET SWITCH WITH VLAN
16
FIREWALL
2
1
27
28
2
3
30
38
36
SENSE
40
14
CONTROLLER
24
PUBLIC NETWORK
10

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05086

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H02H 3/05; H04L 1/22; G06F 15/177
US CL : 714/48, 47; 713/201; 709/220,221,224,249
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 714/48, 47; 713/201; 709/220,221,224,249

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PLUS, STN, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	UA 5,802,320 A [BEAHR et al.] 01 September 1998, see abstract, fig.5, col.3, line 15 through col.6, line 18, col.7, line 12 through col.8, line 68, col.9, line 8 through col.10, line 45	1-28
Y	US 5,790,548 A [SISTANIZADED et al.] 04 August 1998, see abstract, fig.10, col.1, lines 62-68, col.8, lines 3-9, col.12, lines 3-20	1-28
A	US 5,473,599 A [LI et al.] 05 December 1995, see entire document	1-28
A	US 5,287,461 A [MOORE] 15 February 1994, see entire document	1-28

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 JUNE 2000	Date of mailing of the international search report 27 JUN 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DIEU-MINH LE Telephone No. (703) 305-9408

Form PCT/ISA/210 (second sheet) (July 1998) *

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05086

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,432,907 A [PICAZO, Jr. et al.] 11 July 1995, see entire document	1-28
A	US 5,781,715 A [SHEU] 14 July 1998, see entire document	1-28